==========
H I P A A n o t e -- Volume 2, Number 35 – September 11, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
==========

PUTTING THE PRIVACY CHANGES TO WORK:
A "How-To" Guide to the August 2002 HIPAA Privacy Rule Modifications
60-minute audio conference + slides

** Wednesday, September 25 at 2:00 PM **

For more information or to register, go to:
http://www.HIPAAdvisory.com/ezcart/index.cfm

==========

*** Biometrics: Their Potential Role in HIPAA Security ***

In information technology, biometrics refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, for authentication purposes. Basically, biometric technology can be applied in situations that ask "Who are you?"

In recent years, healthcare organizations have begun to explore biometric solutions as an alternative to the conventional password. There is nothing that can be borrowed, stolen, or forgotten; and forging one biometric characteristic is practically impossible. Biometrics are fast, reliable, secure, convenient and highly accurate. They are increasingly viewed as an effective means of managing access to information systems, preventing the unauthorized use of system resources, and ensuring higher security of financial and patient records - all critical to meeting HIPAA security requirements.

For the most part, existing biometric technologies function similarly. For example, biometrics information is collected by scanning an individual's hand or face, or by recording an individual's voice. The information then is converted into mathematical data that can be compared against an existing database, authenticating or refuting the individual's identity.

Biometrics are widely viewed as a major wave in the future of security protections. International Biometric Group reports in its Biometric Market Report 2003, that

* Finger-scan and biometric middleware will emerge
  as two critical technologies for the desktop,
  together comprising approximately 40 percent of
  the biometric market by 2005;

* New service models will dominate the field, leveraging

a burgeoning biometric infrastructure comprised of finger-scan readers, telephones, signature tablets, and video cameras.

Despite vendor claims, there is no best biometric technology. However, potential users should be able identify the most accurate, easiest to use, easiest to deploy, or cheapest biometric for a PARTICULAR deployment. Nor is biometric technology perfect. Potential drawbacks of biometrics usage are that users will feel de-humanized or intruded upon, biometric devices (specifically fingerscan) may be problematic for certain individuals (ie. staff with arthritic hands), and environmental factors can impede or compromise the accuracy of results, if not properly considered before deployment. But biometrics can offer major advantages over traditional password practices, including increased security support, in a variety of traditional healthcare situations.

For example, currently many healthcare users, like physicians and other providers, are given generic passwords. After HIPAA, covered entities with generic passwords will not be compliant. Biometric applications can enable each person with access to patient data to have a unique identity so that his or her database activity can be monitored. Similarly, frequent use of agency nurses and other temporary staff has resulted in organizations allowing staff to share passwords. After HIPAA, covered entities that allow shared passwords will not be compliant. Use of fingerscans or other biometric authentication, in conjunction with a user name, may be a viable alternative for eliminating such situations.

Biometrics also offers a significant return on investment (ROI) for organizations that have implemented stringent password management practices. ROI can be achieved through:

* Reducing time and resources required to administer user IDs and passwords, and required at the help desk for security access issues;

* Minimizing productivity time lag incurred when new employees are hired and need to be provided with specific resources to perform their duties;

* Eliminating or reducing the possibility of a major breach of security due to insufficient user access control.

A biometric solution that is appropriate to a particular healthcare environment will enhance security, reduce administrative cost required to manage passwords, and reduce password confusion and frustration. Consider investigating biometric solutions to help meet your organization's HIPAA security needs.

Josef Spencer, Director
Phoenix Health Systems

For more...

* on the HIPAA security standards, go to:
http://www.hipaadvisory.com/regs/securityandelectronicsign/

* technology-related information, go to:
  http://www.hipaadvisory.com/tech/

That's today's HIPAAnote...now, pass it along!

==========

Bring your HIPAA questions and ideas to life at... HIPAAlive!

Join nearly 5,000 other thinkers, planners, learners and lurkers who are already members of our sister email discussion list. We almost make HIPAA fun! Almost. (Also available in a PREMIUM version of easy-to-navigate, individually formatted, "cleaned up" digests.) Now when you join HIPAAlive-Premium, you receive a FREE Doc Site Membership!

Find out more about HIPAAlive, the Doc Site, and HIPAAlive-Premium at:
http://www.HIPAAdvisory.com/live

==========

HIPAAnotes are published weekly as a learning tool to help you and your associates stay tuned-in to HIPAA and its implications. Forward it to anyone with a "need to know" through your own internal mailing list, intranet or newsletter -- whatever works for you...

Our HIPAAcratic oath: We'll use your ideas for HIPAAnotes -- send them!
Email D'Arcy Gue, Editor: info@phoenixhealth.com
==========
You are currently subscribed to hipaanotes as: kmckinst@dmhhq.state.ca.us

To unsubscribe, send an email to: leave-hipaanotes-16283428V@lists.hipaalert.com
---
List archives:
http://www.hipaadvisory.com/notes/archives.htm
==========